



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/788,566	02/21/2001	TsuneYuki Kikuchi	Q63195	5930
7590 09/02/2008 SUGHRUE, MION, ZINN, MACPEAK & SEAS 2100 Pennsylvania Avenue, N.W. Washington, DC 20037				
EXAMINER CHANKONG, DOHM				
ART UNIT 2152		PAPER NUMBER		
MAIL DATE 09/02/2008		DELIVERY MODE PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

# Office Action Summary

**Application No.**

09/788,566

**Applicant(s)**

KIKUCHI, TSUNEYUKI

**Examiner**

DOHM CHANKONG

**Art Unit**

2152

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 28 May 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 3-9, 11, 14-20 and 22-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 3-9, 11, 14-20, and 22-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/C)
- Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. This action is in response to Applicant's arguments filed on 5/28/2008. Claim 30 is added. Claims 3-9, 11, 14-20, and 22-30 are presented for further examination.
2. This is a final rejection.

### ***Response to Arguments***

3. With respect to the independent claims, Applicant argues that Abraham does not teach or suggest a packet monitor device configured to monitor a service identifier of said packets. Applicant argues that Abraham are directed towards identifying information using the file transfer protocol. Contrary to Applicant's assertions, Abraham does suggest monitoring a service identifier where the identifier is control data for identifying a service which the server provides to a user.

It should first be noted that Abraham discloses one purpose of his invention is to allow administrators to "set specific rules for the users of the computers connected to the LAN 44 regarding what type of services...on the Internet 40 to which any user may have access" [column 6 «lines 28-31»]. This citation is relevant because it would clearly suggest to one of ordinary skill in the art the need to discern which services a user is attempting to access in order to be able to set specific rules for those services. Thus, "if a rule denies a user access to a particular service or type of information, any IP packets from that user requesting access for that service...will not be allowed to pass" [column 6 «lines 31-35»]. Clearly, Abraham is implying the need to monitor IP packet and determine from the packet the service that a user is requesting.

Abraham accomplishes these monitoring and determination functions by inferring the services through the type of protocols being used by a particular packet. So for example, if an administrator wished to block access to the internet, Abraham teaches blocking packets that use the HTTP protocol [Fig. 8L | column 23 «lines 10-29»]. Abraham's reliance on determining the use of the HTTP protocol by a packet to infer a user's service request for the Internet reads on Applicant's use of the service identifier. Since Applicant's service identifier is merely "control data for identifying a service" and Abraham discloses utilizing specific protocols (HTTP) to identify a particular service (the Internet), Abraham teaches the service identifier as claimed. For email services, Abraham discloses determining whether the packets contain SMTP, POP2, or POP3 information [column 12 «lines 3-6»]. Abraham therefore is monitoring packets for control data, such as SMTP data, and infers that an email service is requested from this control data.

Based on the foregoing discussion, Applicant's arguments with respect to the independent claims are not persuasive. The rejections set forth in the previous action are therefore maintained.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 3, 6-9, 11, 14, 17-20 and 22-25 are rejected under 35 U.S.C §103(a) as being unpatentable over Abraham et al, U.S Patent No. 5.983.270 ["Abraham"], in view of Nickles, U.S Patent No. 6.134.591.

5. As to claim 1, Abraham discloses a system for monitoring packets transmitted on a channel connecting an application server and an end-user of said application server to each other, said system comprising:

a certification server which certifies the end-user [column 5 «line 63» to column 6 «line 4»]; and

a packet monitor device which, on receipt of a request from said certification server, monitors packets transmitted on said channel [column 1 «lines 13-17» | column 7 «lines 51-67»], wherein said certification server includes:

a first memory which stores a user management table including ID numbers of end-users, a monitoring parameter designating a packet to be monitored, a threshold parameter designating a method of monitoring said packet [Figures 9D, 17, 25A, 25B : notify rule, log rule | column 15 «lines 35-40»]; and

a second device which transmits a request to said packet monitor device to start or finish monitoring said packet at a timing when said end-user logs-in or logs-out the terminal [column 9 «lines 1-10»];

wherein said packet monitor device includes:

a fourth memory which stores a first time at which a packet transmitted from one of

said application server and said user arrives, when said packet monitor device receives a request from said second device to monitor said packet [Figure 20 | column 47 «lines 14-24» | see also response to arguments above];

an analyzer which monitors a second time at which packets meeting said monitoring parameter arrive, and determines whether any rule has been satisfied during an interval between said first time and said second time [column 7 «lines 51-67» | column 9 «lines 51-65» | column 47 «lines 14-24» | column 41 «line 53» to column 42 «line 42»]; and

an annunciator which makes annunciation to said user when a certain rule is satisfied during said interval [Figure 26 | column 11 «lines 53-64» | column 13 «lines 62-67»]; and

wherein said packet monitor device is configured to monitor at least one of a data sequence of said packets, a service identifier of said packets [Figure 8J | column 21 «lines 39-50» : protocol ID identifies the type of service – for example, email, web, or FTP], and a checksum of said packet.

Abraham does not expressly disclose storing a password in the table. However such a feature was well known in the art at the time of Applicant's invention. Abraham does disclose storing user's information, including the user's ID and access level [column 16 «lines 6-9»]. Additionally, as is well known in the art, Abraham also discloses the feature whereby a user logs on to his terminal using a password [column 5 «lines 63-67» | see also response to arguments above]. In a related field of invention, Nickles discloses a management database that stores usernames with their respective passwords for the same purpose as Abraham [Figure 7 «item 708a» | column 6 «lines 7-17»]. Therefore it would have been obvious to one of ordinary skill in the art to have reasonably inferred that Abraham's management table would contain passwords.

Such a feature is implied by Abraham because he teaches that a user is monitored only after logging into the LAN. One of ordinary skill in the art would understand this to include submitting a user ID and a password as is well known in the art. Thus, passwords are stored with user IDs, as further evinced by Nickles.

6. As to claim 3, Abraham discloses:

a fourth memory which stores a first time at which a packet transmitted from one of said application server and said user arrives, when said packet monitor device receives a request from said second device to monitor said packet [Figure 20 | column 47 «lines 14-24»];

an analyzer which monitors a second time at which packets meeting said monitoring parameter arrive, and determines whether any rule has been satisfied in an interval in said second time [column 7 «lines 51-67» | column 9 «lines 51-65» | column 47 «lines 14-24»]; and

an annunciator which makes annunciation to said user when there is a certain rule in said interval [Figure 26 | column 11 «lines 53-64» | column 13 «lines 62-67»].

7. As to claim 6, Abraham discloses the packet monitor device including:

a second memory which stores said monitoring parameter transmitted from said second device [column 7 «lines 22-50»];

a third memory which stores said threshold parameter transmitted from said second device [column 2 «lines 47-53» | column 7 «lines 22-50»]; and

a third device which said third and fourth memories when said second device transmits a request to said packet monitor device to start or finish monitoring said packet [column 6 «line 60» to column 7 «line 3» | column 7 «lines 22-50» | column 47 «lines 5-24»].

8. As to claim 7, Abraham discloses the analyzer analyzing whether there is any rule in said interval and whether said interval exceeds said threshold parameter [column 11 «lines 53-64»], and said annunciator makes annunciation to said end-user when said analyzer judges that there is a certain rule in said interval and that said interval exceeds said threshold parameter [column 13 «lines 53-60»].

9. As to claim 8, Abraham discloses a method of monitoring packets transmitted on a channel connecting an application server and an end-user of said application server to each other, comprising the steps of:

acquiring a monitoring parameter indicative of a packet to be monitored, when said end-user logs-in his/her terminal [column 5 «line 63» to column 6 «line 4»];

monitoring a time at which packets coincident with said monitoring parameter arrive, and determining whether there is any rule in an interval between a time when the monitoring parameter is acquired said arrival time [column 7 «lines 51-67» | column 11 «lines 53-64» | column 41 «line 53» to column 42 «line 42»];

making annunciation to said end-user when there is a certain rule in said interval [column 13 «lines 61-67»]; and



monitoring at least one of a data sequence of said packets, a service identifier of said packets [Figure 8J | column 21 «lines 39-50» : protocol ID identifies the type of service – for example, email, web, or FTP], and a checksum of said packet;

wherein said monitoring parameter is included in a user management table which further includes an ID number of said user and a threshold parameter designating a method of monitoring said packet [Figures 9D, 17, 25A, 25B : notify rule, log rule | column 15 «lines 35-40»], and said step includes the steps of:

retrieving said user management table, based on said ID number input by said end-user [column 8 «lines 13-25» | column 16 «lines 12-19» : user must log in to the LAN before monitoring begins – process of logging in submits his user ID];

acquiring said monitoring parameter, if said monitoring parameter is stored in said user management table [Figure 17 : user rules]; and

acquiring said threshold parameter, if said threshold parameter is stored in said user management table [Figures 17, 25B : user policies such as quota limit | column 34 «lines 11-58»].

Abraham does not disclose storing a password related to the users. However such a feature was well known in the art at the time of Applicant's invention. Abraham does disclose storing user's information, including the user's ID and access level [column 16 «lines 6-9»]. Additionally, as is well known in the art, Abraham also discloses the feature whereby a user logs on to his terminal using a password [column 5 «lines 63-67»]. In a related field of invention, Nickles discloses a management database that stores usernames with their respective passwords for the same purpose as Abraham [Figure 7 «item 708a» | column 6 «lines 7-17»]. Therefore it

would have been obvious to one of ordinary skill in the art to have reasonably inferred that Abraham's management table would contain passwords. Such a feature is implied by Abraham because he teaches that a user is monitored only after logging into the LAN. One of ordinary skill in the art would understand this to include submitting a user ID and a password as is well known in the art. Thus, passwords are stored with user IDs, as further evinced by Nickles.

10. As to claim 9, Abraham discloses ceasing monitoring when said end-user logs-out his/her terminal [column 8 «lines 23-25»].

11. As to claim 11, Abraham discloses the step including the step of analyzing whether there is a certain rule in said interval and whether said interval exceeds said threshold parameter, after acquiring said threshold parameter and said step includes the step of making annunciation to said end-user, if there is a certain rule in said interval and said interval exceeds said threshold parameter [column 11 «lines 53-64» | column 13 «lines 53-60»].

12. As to claims 14, 17, and 18, as they are merely mediums that store the system of claims 3, 6, and 7, respectively, they do not teach over the claimed limitations. Therefore claims 14, 17, and 18 are rejected for the same reasons set forth for claims 3, 6, and 7, supra.

13. As to claims 19 and 20, as they are merely mediums that store the system of claims 8 and 9, respectively, they do not teach over the claimed limitations. Therefore claims 19 and 20 are rejected for the same reasons set forth for claims 8 and 9, supra.

14. As to claims 21 and 22, as they are merely mediums that store the system of claims 10 and 11, respectively, they do not teach over the claimed limitations. Therefore claims 21 and 22 are rejected for the same reasons set forth for claims 10 and 11, *supra*.

15. As to claims 23 and 24, Abraham discloses the end-user is not performing an administrative function of said application server [column 5 «line 63» to column 6 «line 4» : difference between client computers and administrative computers | column 16 «lines 12-16»].

16. As to claim 25, Abraham discloses the packet monitor is located in the channel between the application server and the end-user [Figure 2 «item 50»].

17. As to claim 26, Abraham discloses said packet monitor device is configured to compare information about said packets to said monitoring parameter [column 45 «lines 1-31» : determining whether the intercepted packets match any of the user-defined rules. Matching packets imply that the information about said packets is compared to the rules].

18. As to claim 27, Abraham discloses a counter, wherein said counter is configured such that, if said rule is satisfied, then said counter is incremented [column 14 «lines 32-40» | column 46 «lines 11-24» | column 48 «lines 41-54» where : Abraham's log reads on Applicant's claimed counter. Every time a rule matches a rule, the log is updated to indicate the match. In this way, the log provides a count of the packets that matched the monitoring rule].

19. As to claim 28, Abraham discloses a comparator, which compares said counter to said threshold parameter [column 49 «lines 1-22» where : the count in the log table is compared with a quota threshold].

20. As to claim 29, Abraham discloses said threshold parameter comprises a duration after which a packet coincides with the monitoring parameter [column 40 «lines 20-34» : predetermined time interval] or a service fee.

21. Claims 4, 5, 15 and 16 are rejected under 35 U.S.C §103(a) as being unpatentable over Abraham in view of Engel et al, U.S Patent No. 6.115.393.

22. As to claim 4, Abraham discloses a system for monitoring packets transmitted on a channel connecting an application server and an end-user of said application server to each other, said system comprising:

a certification server which certifies the end-user [column 5 «line 63» to column 6 «line 4»]; and

a packet monitor device which, on receipt of a request from said certification server, monitors packets transmitted on said channel [column 1 «lines 13-17» | column 7 «lines 51-67»],

wherein said certification server includes:

a first memory which stores a user management table including ID numbers of end-users, a monitoring parameter designating a packet to be monitored, a threshold

parameter designating a method of monitoring said packet [Figures 9D, 17, 25A, 25B :  
notify rule, log rule | column 15 «lines 35-40»];

a second device which transmits a request to said packet monitor device to start or finish  
monitoring said packet at a timing when said end-user logs-in or logs-out the terminal [column 9  
«lines 1-10»]; and

wherein said packet monitor device monitors an interval between which packets arrive at  
said end-user from said application server and vice versa [column 9 «lines 56-65»], and said  
certification server makes annunciation to said end-user [column 13 «lines 61-67»], and

wherein said packet monitor device is configured to monitor at least one of a data  
sequence of said packets, a service identifier of said packets [Figure 8J | column 21 «lines 39-50»  
: protocol ID identifies the type of service – for example, email, web, or FTP], and a checksum  
of said packet.

Abraham does not disclose that the monitoring and threshold parameters are updated by  
instruction of the end-user. However, such a feature was well known in the art at the time of  
Applicant's invention. For example, Engel discloses a network monitoring system. Engel  
discloses that monitoring and threshold parameters that dictate what packets are to be monitored  
are controlled by an end-user [column 30 «line 55» to column 31 «line 13»]. It would have been  
obvious to one of ordinary skill in the art to modify Abraham to include Engel's functionality.  
One would have been motivated to provide such functionality to enable all network users to  
modify parameters associated with the monitors of a network; this capability is "normally the  
prerogative of the system administrator" and thus Engel's teachings would benefit Abraham's  
network monitoring system.

23. As to claim 5, Abraham discloses the packet monitor device including:

a second memory which stores said monitoring parameter transmitted from said second device [column 7 «lines 22-50»];

a third memory which stores said threshold parameter transmitted from said second device [column 2 «lines 47-53» | column 7 «lines 22-50»]; and

a third device which said third and fourth memories when said second device transmits a request to said packet monitor device to start or finish monitoring said packet [column 6 «line 60» to column 7 «line 3» | column 7 «lines 22-50» | column 47 «lines 5-24»].

24. As to claims 15 and 16, as they do not teach or further define over previously claimed limitations, they are rejected for at least the same reasons set forth for claims 4 and 5, respectively.

25. Claim 30 is rejected under 35 U.S.C. §103(a) as being unpatentable over Abraham and Nickles, in view of Applicant's admitted prior art ["admitted art"].

26. As to claim 30, while Abraham does disclose services such as email and the Internet [Figure 8L], Abraham does not expressly disclose that such services are provided for a fee. However, providing services such as email or internet access for a fee was a well known feature in the art at the time of Applicant's invention. For example, Applicant's admitted art discloses that service providers typically employ service fees for using email or the Internet. Therefore it

would have been reasonable for one of ordinary skill in the art to have inferred that Abraham's services were provided for a fee as taught by Applicant's admitted art. It would have been obvious for one of ordinary skill in the art because service fees are a valuable way for service providers to make a profit.

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to DOHM CHANKONG whose telephone number is (571)272-3942. The examiner can normally be reached on Monday-Friday [8:30 AM to 4:30 PM].

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571.272.3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Dohm Chankong/  
Examiner, Art Unit 2152

/Bunjod Jaroenchonwanit/  
Supervisory Patent Examiner, Art Unit 2152



**Application Number****Application/Control No.**

09/788,566

**Applicant(s)/Patent under  
Reexamination**

KIKUCHI, TSUNEYUKI

**Examiner**

DOHM CHANKONG

**Art Unit**

2152